IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AON ESOLUTIONS, INC. 200 East Randolph Street Chicago, IL 60601 Plaintiff, v. STEPHEN BRESLIN 1309 E. Berks Street Philadelphia, PA 19125, JAMES HAAS S97 W13169 Champions Drive Muskego, WI 53150, GINA ROTHWEILER 927 Jeannette Street Des Plaines, IL 60016, AND RISKONNECT, INC. 30 South Park Square, Suite 202 Marietta, GA 30060, Defendants.	)	CIVIL ACTION NO. 2:11-cv-05050-JCJ

REPLY BRIEF IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

I. INTRODUCTION

Defendants demonstrated in their Motion to Dismiss and accompanying Memorandum of Law ("Defendants' Brief") that Plaintiff's Computer Fraud and Abuse Act ("CFAA") Cause of Action should be dismissed with prejudice. In response, Plaintiff asserts in its Memorandum of Law ("Response Brief") that it has sufficiently stated a claim because, although Mr. Breslin, Mr. Haas, and Ms. Rothweiler (the "individual Defendants") were granted permission to obtain Plaintiff's information, they unlawfully used it by duplicating it in violation of Plaintiff's

Information Security Policy. However, rather than warranting denial of Defendants' Motion, this allegation of "misuse" is insufficient to sustain a cause of action under 18 U.S.C. § 1030(a)(4), Defendants' Motion to Dismiss should be granted.

Moreover, even assuming that Plaintiff stated a claim upon which relief may be granted, this Court should nevertheless decline supplemental jurisdiction over Plaintiff's state law claims because they substantially predominate the CFAA claim. *See,* Defendants' Brief at 10.

II. ARGUMENT

1. The Individual Defendants Acted With Authorization when they Accessed Aon's Computers Because they Had Permission to Do So

Plaintiff concedes that the individual Defendants were authorized to access Plaintiff's computers and view its confidential information. To adequately plead a CFAA claim that the individual Defendants accessed a protected computer "without authorization," Plaintiff must allege that the individual Defendants acted without permission when they accessed and viewed confidential information on Plaintiff's computers. *See*, Defendants' Brief at 4. Further, Plaintiff must allege that the employees hacked into a protected computer, or otherwise engaged in conduct analogous to breaking and entering. *See*, *id. See also, Brett Senior & Assoc., P.C. v. Fitzgerald,* No. 06-1412, 2007 WL 2043377, at *3 (E.D.Pa. July 13, 2007) (finding that, to violate the CFAA, defendant must have trespassed onto a protected computer or have committed computer theft); *Consulting Professional Resources, Inc. v. Concise Technologies LLC*, No. 09-1201, 2010 WL 1337723, at *5 (W.D.Pa. March 9, 2010) (concurring with those courts that have "observed that the statute was enacted to create a cause of action against 'hackers,' rather than disloyal employees").

Plaintiff attempts to avoid dismissal by arguing "agency law" controls authorization. Plaintiff's Response at p. 6-7. This Court has rejected the use of agency law to interpret the "without authorization" language of § 1030(a)(4). "[Plaintiff's] view—that authorization turns on the purpose for which an employee accesses a computer rather than the employer's actions to permit or restrict such access-has been rejected by numerous courts, including courts in this District." *Grant Mfg. & Alloying, Inc. v. McIlvain*, No. 10-1029, 2011 WL 4467767, at *6 (E.D.Pa. September 23, 2011). *See also*, *Bro-Tech Corp. v. Thermax, Inc.*, 651 F.Supp.2d 378, 406, 407 (E.D.Pa. 2009) (declining to adopt Plaintiff's use of agency law); *Consulting Professional Resources,* 2010 WL 1337723, at *4-6 (rejecting *Citrin* and "declin[ing] to construe the CFAA by reliance upon agency principles..."); *U.S. v. Nosal,* 642 F.3d 781, 786 (9th Cir. 2011) ("reject[ing] the *Citrin* approach as inconsistent with our conclusion that... it is the action of the *employer* that determines whether an employee is authorized..."). Thus, Plaintiff's reliance on agency principles to determine whether the individual Defendants' access was "without authorization" is misplaced.

Two compelling reasons counsel against deviating from prior holdings in this District by adopting an interpretation of "without authorization" predicated upon agency law. First, the incorporation of agency principles is contrary to the rule of lenity, which "require[s] the Court to favor the narrower interpretation of [§ 1030(a)(4)]..." *Brett Senior*, 2007 WL 2043377, at *4. Second, this approach is contrary to the text of § 1030(a)(4): because Plaintiff's interpretation prohibits using information against the interests of the employer, it improperly conflates "access" to information with "use" of information. *Consulting Professional Resources,* 2010 WL 1337723, at *4-6.

2. The Individual Defendants did not Exceed Authorization Because Misuse or Misappropriation of Information is not a Violation of § 1030(a)(4) and Because the Information Security Policy is not an Access Restriction

The individual Defendants did not exceed their authorized access. As defined by the statute, "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C.A. § 1030(e)(6). Although the Third Circuit has not interpreted this language, this Court has found that

> "[w]hether an employee has exceeded authorized access depends on the computer access restrictions imposed by his employer. Where an employer places limitations on the computer information an employee is entitled to obtain or alter or the manner in which the employee is entitled to obtain or alter such information, and notifies employees of such limitations, an employee who runs afoul of the limitations exceeds his authorized access under the CFAA."

Grant Mfg., 2011 WL 4467767, at *7. Because Plaintiff has not alleged that the individual Defendants exceeded any access restrictions, Plaintiff's claim should be dismissed.

Plaintiff has alleged neither that it has imposed any access restrictions nor that the individual Defendants ran afoul of such limitations. Plaintiff's Complaint admits that the individual Defendants were authorized to *obtain* Plaintiff's confidential information (*See*, Complaint ¶ ¶ 12, 16, 20) and alleges only that they wrongfully *used* the information by duplicating it. *See,* Complaint ¶ ¶ 15, 19, 23. Plaintiff now argues in its Response Brief[1] that the individual Defendants improperly "stored" this information on their personal computers in

[1] Because Plaintiff has not pled that any Defendant violated its Information Security Policy and that such a violation is grounds for liability under § 1030(a)(4), this Court should disregard allegations related thereto raised only the Response Brief. "While counsel may 'clarify' a pleading through subsequent briefing, a lawyer's statement in a response brief is no substitute for adequately pleaded facts in a complaint, and a memorandum cannot provide allegations that are wholly absent from the... Complaint." *In re PHP Healthcare Corp.*, 128 Fed. Appx. 839, 847 (3rd Cir. 2005).

violation of Plaintiff's Information Security Policy, and, again, that this "duplication... therefore exceeded their access to Aon's computers..." Response Brief at 12. However, the Policy language quoted by Plaintiff regulates only the use (*i.e.*, copying) of information once access has been obtained with permission. As such, Plaintiff has alleged the existence and violation of *use* restrictions, but not *access* restrictions. Although Plaintiff may have identified a basis for a state law breach of contract claim, a mere breach of contract does not rise to the level of a Federal offense under CFAA § 1030(a)(4), unless the contract restricts *access*. Here, at best, the Policy attempts to restrict misuse or misappropriation, not access.

Moreover, a CFAA § 1030(a)(4) claim cannot be based solely on allegations that the employee misused or misappropriated information. "The conduct targeted by section (a)(4)... is the unauthorized procurement or alteration of information, not its misuse or misappropriation." *Brett Senior*, 2007 WL 2043377, at *3. *See also*, Defendants' Brief at 5-9 (arguing that misuse or misappropriation alone is insufficient to support a CFAA claim). Although Plaintiff would have this Court interpret § 1030(a)(4) as creating liability for an employee's violation of mere use restrictions, this Court has rejected such an approach in several cases.

For example, this case is indistinguishable from *Consulting Professional Resources*. In that case, the plaintiff accused an employee of wrongfully duplicating confidential information for a competitor in violation of an employment agreement. Because the plaintiff admitted that it authorized the defendant to access its computers and obtain its confidential information, this Court held that the plaintiff

> "does not allege that [defendant] accessed its computer without authorization or that her access exceeded her authorized access, rather it argues that [defendant's] *eventual use* of the information accessed violated her employment contract. While disloyal employee conduct might have a remedy in state law, the reach of the CFAA does not extend to instances where the employee was authorized to access the information he later utilized to the possible detriment of his former employer."

Consulting Professional Resources, 2010 WL 1337723 at *6 (emphasis added). Plaintiff here likewise admits that the individual Defendants were authorized to access all of the confidential information that they were accused of unlawfully duplicating and as such Plaintiff does not and cannot allege that they did so without authorization or in excess thereof.

This Court's holding in *Brett Senior* similarly makes clear that the individual Defendants did not exceed their authorization. As is precisely the case here, in *Brett Senior* the plaintiff accused the defendant of violating the terms of his employment contract by attaching an external hard drive to the plaintiff's computer and duplicating confidential information. That the plaintiff in *Brett Senior* "conceded that there was nothing *per se* actionable" (Response Brief at 10) about duplicating information is not dispositive here because it does not clarify which acts are *per se* actionable. Immediately following the language cited by Plaintiff, this Court clarifies that "[b]ecause there is no allegation that [defendant] lacked authority *to view* any information in the [plaintiff's] computer system, the CFAA claim fails." *Brett Senior*, 2007 WL 2043377, at *3 (emphasis added). "[Defendant]... cannot be liable... unless he, at a minimum, trespassed into [Plaintiff's] computer system. [L]awfulness of... entry defeats the CFAA claim." *Id.* Here, because Plaintiff admits that the individual Defendants were granted authority to view Plaintiff's confidential information and because the Information Security Policy limited only the authority to use that information once viewed, Plaintiff's CFAA claim similarly fails.

Cases cited by Plaintiff do not support an interpretation of § 1030(a)(4) as criminalizing a violation of an employer's use restrictions without any contemporaneous violation of an access restriction. For example, Plaintiff cites *U.S. v. Tolliver*, No. 10-3439, 2011 WL 4090472 (3d Cir.

Sep. 15, 2011)[2] for the proposition that "employees who use work computers to access information in violation of set policies are in violation of the CFAA." Response Brief at 10. However, in *Tolliver* the government established that its employee had violated an access restriction which mandated that "employees were not permitted to *look at* a customer's account... without a business purpose." *Tolliver*, 2011 WL 4090472, at *2 (emphasis added). Likewise, in *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), Rodriguez's conviction was upheld because he accessed his employer's computer even though he was "not authorized *to obtain* personal information for nonbusiness reasons." *Rodriguez*, 628 F.3d at 1263 (emphasis added). Similarly, the defendants in *Nosal* faced CFAA liability because they violated "a computer use policy that placed... restrictions on the employees' *access* both to the system and to the Searcher database in particular." *Nosal*, 642 F.3d at 787 (emphasis added). In each of these cases, the employer's use restrictions were *also* access restrictions because they limited the employee's permission to view and obtain information if the employee did so with an improper purpose. Because Plaintiff does not allege that its Information Security Policy similarly limits an employee's permission to view information, its CFAA claim fails.

This Court should not hold that solely violating an employer's restrictions on use of information creates liability under the CFAA. First, even if Plaintiff and Defendants present equally plausible interpretations of § 1030(a)(4) and § 1030(e)(6), the rule of lenity requires the court to favor Defendants' narrower interpretation. *See*, Defendants' Brief at 8; *Brett Senior*, 2007 WL 2043377, at *10. Second, the statute as a whole indicates that Congress did not intend

[2] Plaintiff mischaracterizes the holdings of *Tolliver*. First, the court did not consider *Citrin* or any similar case relying on agency law, let alone affirm them. Second, the court devoted very little text to the CFAA issue and the impact of its holding on this case is not clear. Third, as is true of every case cited by Plaintiff, the court interpreted another provision of the CFAA rather than § 1030(a)(4).

to create liability for improper use of information. *See, Orbit One Communications, Inc. v. Numerex Corp.*, 692 F.Supp.2d 373 (S.D.N.Y. 2010) (noting that statutory definitions of "damage" and "loss" indicate that Congress intended to target computer hacking and not misuse of information). Third, Plaintiff's interpretation improperly conflates "access" of a computer with "use" of information. *Consulting Professional Resources,* 2010 WL 1337723, at *6. However, "a violation [of § 1030(a)(4)] does not depend upon the defendant's unauthorized use of *information,* but rather upon the defendant's unauthorized use of *access.*" *Diamond Power Intern., Inc. v. Davidson*, 540 F.Supp.2d 1322, 1343 (N.D.Ga. 2007). Because § 1030(e)(6) prohibits "access[ing] a computer... to obtain or alter information," and because an employee must have obtained information before they can misuse it, Plaintiff's conflation of "access" and "use" produces an absurd and circular result whereby an employee is prohibited from using the employer's information in such a way so as to obtain the very same information that the employee is accused of misusing. Therefore, this Court should reject an interpretation prohibiting only misuse of information.

3. Even Assuming Plaintiff Stated a Claim for which Relief may be Granted, this Court Should Decline Supplemental Jurisdiction

As permitted by 28 U.S.C. § 1367(c)(2), this Court should decline supplemental jurisdiction because Plaintiff's state law claims substantially predominate its sole federal claim. Defendants have cited case law directly on-point demonstrating that Plaintiff's CFAA claim is merely an appendage to its state law claims, which form the real body of the case. *See*, Defendants' Brief at 10. Thus, even if this Court does not dismiss Plaintiff's CFAA Cause of Action for failure to state a claim, it should dismiss Plaintiff's state law causes of action.

III. CONCLUSION

For the foregoing reasons, Defendants[3] respectfully request that their Motion to Dismiss be granted.

Submitted this 9th day of November, 2011.

COCHRAN & EDWARDS, LLC

/s/ Randy Edwards
RANDY EDWARDS (pro hac vice)
Georgia Bar No. 241525
randy@cochranedwardslaw.com
2950 Atlanta Road SE
Smyrna, GA 30080
Tel.: 770-435-2131
Fax: 770-436-6877

and

KLEHR HARRISON HARVEY BRANZBURG LLP

/s/ Frank M. Correll, Jr.
Frank M. Correll, Jr.
Matthew J. Borger
1835 Market Street, Suite 1400
Philadelphia, PA 19103
Tel.: 215-569-4094
Fax: 215-568-6604
E-mail: fcorrell@klehr.com

Counsel for Defendant Riskonnect, Inc.

GERMAN GALLAGHER & MURTAGH

/s/ Dean F. Murtagh
Dean F. Murtagh
200 South Broad Street, 5th Floor
Philadelphia, PA 19102
Tel.: 215-545-7700
Fax: 215-732-4782
E-mail: murtaghd@ggmfirm.com

and

GASS WEBER MULLINS LLC

/s/ Michael B. Brennan
Michael B. Brennan (pro hac vice)
Daniel J. Kennedy (pro hac vice)
309 North Water Street, Suite 700
Milwaukee, WI 53202
Tel.: 414-223-33--
Fax: 414-224-6116

Counsel for Defendant James Haas

[3] Contrary to Plaintiff's assertion, Defendant Riskonnect has standing to challenge the CFAA claim because jurisdiction over Riskonnect is predicated upon it. Regardless, because the Motion to Dismiss is joined by all Defendants, this issue is moot.

BLANK ROME LLP

/s/ Leigh Ann Buziak
Anthony B. Haller
Leigh Ann Buziak
One Logan Square
130 N. 18th Street
Philadelphia, PA 19103
Tel.: 215-569-5500
Fax: 215-569-5555
E-mail: haller@blankrome.com
E-mail: lbuziak@blankrome.com

Counsel for Defendant Stephen Breslin

/s/ Gina Rothweiler (pro se)
Gina Rothweiler
927 Jeannette Street
Des Plaines, IL 60016

CERTIFICATE OF SERVICE

I, Matthew J. Borger, Esquire, hereby certify that on this 9th day of November 2011, a true and correct copy of the foregoing Reply Brief in Support of Defendants' Motion to Dismiss was served upon the following parties, through their counsel of record, via electronic filing (ECF) and first-class mail:

William J. Leahy, Esquire
LITTLER MENDELSON PC
Three Parkway
1601 Cherry Street
Suite 1400
Philadelphia, PA 19102-1321

Counsel for Plaintiff Aon Esolutions, Inc.

Dated: November 9, 2011

/s/ Matthew Borger
Matthew J. Borger